MYSEA Technology Demonstration

Cynthia Irvine, David Shifflett, Paul Clark, Timothy Levin, George Dinolt
Naval Postgraduate School

Abstract

The MYSEA project has produced an innovative architecture and corrresponding engineering prototype consisting of trusted security services and integrated operating system mechanisms for the protection of distributed multi-domain computing environments from malicious code and other attacks. These security services and mechanisms extend and interoperate with existing workstations, applications and open source operating systems, providing new capabilities for composing secure distributed systems using commercial off-the-shelf (COTS) components. The MYSEA technical demonstration illustrates the MYSEA architecture, as well as the mechanisms for providing multi-domain information protection, trusted path extension and quality of security service.

1. Introduction

The purpose of the Monterey Security Enhanced Architecture (*MYSEA*, pronounced, `my-SEE-ah`) project is to provide a trusted distributed operating environment for enforcing multi-domain security policies, which supports unmodified COTS productivity applications. The architecture encompasses a combination of many low-assurance commercial components and relatively few specialized (e.g., high-assurance) multi-domain components. This arrangement permits the ongoing DoD and U.S. Government investment in commodity personal computer (PC) operating systems and applications to be integrated into an environment where enforcement of critical security policies is assigned to more trusted elements. Assurance is derived from the application of high assurance system design and development methods to the trusted elements as well as to the overall architecture.

We feature two demos, which illustrate the following MYSEA characteristics and capabilities:

- A distributed architecture for isolating trusted components in support of commercial and open source applications. The innovative use of add-on components in commercial client-server systems can potentially magnify the impact of trusted open source systems.
- Global and persistent protection of multiple protection domains, such that malicious code may neither exfiltrate confidentially sensitive data, nor corrupt information of higher integrity.
- An open source trusted path mechanism for assured and unambiguous user communication with the trusted computing base.
- Techniques for vertical integration of dynamic security policy control functions with underlying security services in a Quality of Security Service framework [2].

1. MYSEA Domain Separation and Trusted Path Demo

MYSEA is a distributed client-server architecture, the major physical components of which are illustrated in Figure 1:

- Security enhanced servers which provide the locus for security policy enforcement and host various open source or commercial application protocol servers, and
- Security enhanced workstations that consist of commercial-class PCs executing popular commercial software products, along with Trusted Path Extensions that provide trustworthy policy support mechanisms and thus permit server-enforced security policy to be distributed across the network.

The MYSEA Server enforces the security policy and controls access to information. At its heart is a security-enhanced version of the OpenBSD operating system (MYSEOS). Application protocol servers run on the trusted server and provide services and interfaces to shared resources. When MYSEOS is combined with untrusted, but policy constrained (and, in some instances, policy aware) application protocol servers, the result is the MYSEA Server.

Each MYSEA workstation is a PC equipped with a Trusted Path Extension device that provides MYSEA policy support at the workstation. The MYSEA Server(s) and the Trusted Path Extension(s) are the only components directly connected to the physical network. Multiple

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2003	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
MYSEA Technology Demonstration	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Cynthia /Irvine; David /Shifflett; Paul /Clark; Timothy /Levin; George /Dinolt	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Naval Postgraduate School Department of Computer Science Monterey, CA 93943	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**3**	

MYSEA Servers provide scalability within the desired security policy perimeter.

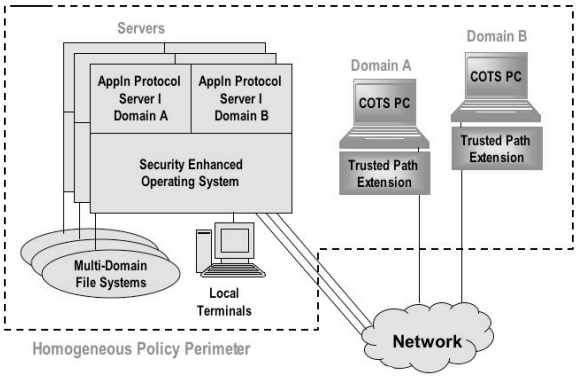

Figure 1. Monterey Security Enhanced Architecture (MYSEA)

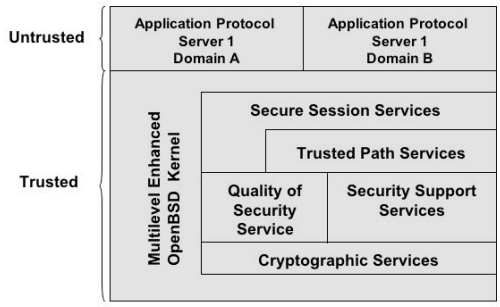

Figure 2. MYSEA server

1.1 Demonstration of Concepts

Using the Trusted Path Extension at the PC, users log on to the MYSEA system by way of a trusted path, establishing an identity for audit and access control purposes, and then establish session attributes such as current sensitivity level. Subsequently, the user can log on to the native client OS at the PC and use standard commercial client software (e.g., web browser or e-mail program) to access applications supported by the MYSEA Server, or use any applications supported by the local PC. From the PC the user can access any domain of server data allowed by the security policy (for example, reading domains of data that are lower in sensitivity than the negotiated level) as well as access local data. By again invoking the trusted path, the user can request to modify session attributes, such as sensitivity level.

1.2 Multi-Domain Policy Enforcement

MYSEOS (depicted in Figure 2) is built on OpenBSD as a set of kernel enhancements to create labeled protection domains and a set of additional security services. The MYSEOS kernel associates security attributes with active and passive entities exported at the operating system interface. Enhancements include a protected security manager configured to interpret these attributes and enforce policy according to configuration-specific rules. An important policy for the MYSEOS kernel to enforce is that malicious code may neither exfiltrate confidentially-sensitive data nor corrupt information of higher integrity; to support this, the MYSEOS kernel provides multi-domain file system support, which provides for the global and persistent separation of data into its respective domains.

1.3 Trusted path extension

The Trusted Path Services component supports multiple locally attached terminals, as well as multiple remote MYSEA workstations. Trusted Path Services maintains the state of the user-to-MYSEA interaction, for example, a user may be logged in with default security attributes, but may not have started a session executing untrusted application code. Trusted Path Services provides an interface to the Security Support Services component to support identification and authentication, negotiation of domain or domain range, password modification, account creation and deletion, and user security attribute maintenance. Once a session has been established, the Trusted Path Services provides a distributed Session Status Database to the Secure Session Services component.

The Trusted Path Extension, under direction from the MYSEA server, supports the following services:

- Secure Attention Key – this service permits users to initiate unambiguous communication with MYSEOS for unspoofable presentation and capture of security critical data at the user interface. The secure attention key must cause a state change in the Trusted Path Extension such that an unforgeable communications path (viz. a *trusted path*) to MYSEOS is established.
- Trusted Path Services – when the trusted path is invoked, the user may elect to input security critical information, such as a password. The trusted path services ensure that prompts from the server are displayed and that an input mechanism for replies is available.
- Controlled LAN Access – provide non-by passable, controlled access to the LAN from the PC. Malicious software on the PC cannot bypass

the Trusted Path.

- Communications and cryptographic services – provide protected communication channels between the server and the Trusted Path Extension. These protected communications are based upon protocols that support both the establishment and maintenance of a trusted path and session-level communications, such as to initiate communication with the server (via the secure attention key), as well as to receive and to respond to commands from the MYSEA Server.
- Negotiated Session Services – these mechanisms ensure trusted *object reuse* at the client PC for both primary and secondary storage. When a user chooses to change domains, certain policies require that information associated with the previous domain be purged from the untrusted PC, e.g. previous session information cannot be reused by subsequent sessions in conflict with the distributed security policy. The Trusted Path Extension ensures that object reuse requirements are met with each session change and as dictated by policy for session level changes. The Trusted Path Extension supports object reuse directives issued by MYSEOS. These directives may include both functional and procedural actions at the workstation.
- Control of Security Critical Activities –control the client and its resources at the time of boot and control security critical actions throughout the client session.

2. Quality of Security Service Demo

MYSEA can be integrated with an external resource or QoS manager to provide a means of dynamically managing its security and performance characteristics. The MYSEA QoSS Manager is the external QoSS interface to MYSEA, and governs security and performance factors of the various MYSEA components, for example, which application protocol servers the client may interact with, and the cryptographic protection characteristics of the underlying communication channels. The QoSS security and connectivity database is managed by the QoSS manager on the MYSEA server, and is distributed to the Trusted Path Extensions, as needed, to modify the protection services afforded an ongoing session.

The Quality of Security Service demonstration shows how decision makers can interact with a QoSS manager to designate the overall security posture of the network. This feature provides the decision maker with a simple set of choices, hiding the underlying complexity of the quality of security service mechanisms [3]. A version of IPsec adapted to provide automated, dynamic Quality of Security Service through the use of an enhanced version of a policy server [1] permits selection of policy-consistent protection mechanisms.

3. Conclusion

MYSEA is a trusted distributed operating environment for enforcing multi-domain security policies that supports unmodified COTS productivity applications. The architecture encompasses a combination of many (untrusted) commercial components and relatively few trusted multi-domain components. Our prototype demonstration illustrates several innovations for protecting multiple data domains and for managing security policies and security services in support of critical applications, including:

- A distributed trusted architecture that utilizes commercial and open source applications to protect and provide access to multiple data domains.
- An open source trusted path mechanism.
- Techniques for vertical integration of security policy control functions with underlying security services.

References

[1] Blaze, Matt, Feigenbaum, Joan, and Keromytis, Angelos D., KeyNote: Trust Management for Public-Key Infrastructures, In Proceedings of the 1998 Security Protocols International Workshop, Springer LNCS vol. 1550, pp. 59 - 63. April 1998, Cambridge, England. Also AT&T Technical Report 98.11.1.

[2] Irvine, C. E., and Levin, T., "Quality of Security Service," in the Proceedings of the New Security Paradigms Workshop, September 2000.

[3] Mohan, Raj, Xml Based Adaptive Ipsec Policy Management In A Trust Management Context, Masters Thesis, Naval Postgraduate School, Monterey, California, September 2002